

Condition and capability of quantum state separation

Yuan Feng,^{1,*} Runyao Duan,^{1,†} and Zhengfeng Ji^{1,‡}

¹*State Key Laboratory of Intelligent Technology and Systems,
Department of Computer Science and Technology, Tsinghua University, Beijing, China, 100084*
(Dated: February 1, 2008)

The linearity of quantum operations puts many fundamental constraints on the information processing tasks we can achieve on a quantum system whose state is not exactly known, just as we observe in quantum cloning and quantum discrimination. In this paper we show that in a probabilistic manner, linearity is in fact the only one that restricts the physically realizable tasks. To be specific, if a system is prepared in a state secretly chosen from a linearly independent pure state set, then any quantum state separation can be physically realized with a positive probability. Furthermore, we derive a lower bound on the average failure probability of any quantum state separation.

PACS numbers: 03.67.Hk, 03.67.Mn

I. INTRODUCTION

A fundamental difference between quantum mechanics and the classical correspondence is that in the former, a system can be not only in a basis state but also in a state which is a linear combination, or ‘superposition’, of different basis states. Quantum computation and quantum information processing benefit extremely from superposition since performing a quantum operation on a superposition is equivalent to performing the same operation synchronously on all of the basis states constituting this superposition. One of the most famous examples is Shor’s quantum factoring algorithm [1]. On the other hand, however, the existence of superposition in quantum mechanics also puts many constraints on the physically realizable information processing tasks, when we have only limited information about the original state of the system that we are concerned with. Take quantum cloning, perhaps the most fundamental task in quantum computation and quantum information processing, as an example. When the state to be cloned is thoroughly known, it can be perfectly cloned by using a state-dependent cloning machine (In fact, since the state is known, we can prepare as many copies of it as needed. The reason behind it is in fact that classical information can be cloned arbitrarily). Here and in the rest of this paper, by ‘perfectly’ we mean the information processing task is realized with certainty and without any approximation or error. Suppose further we want to build a universal cloning machine for different pure states, then only if these states are linearly independent that a desired exact cloning machine exists even in a probabilistic manner [2]. The possibility to obviously clone states from a linearly dependent set is forbidden by the linearity of quantum operations. Another result in Ref. [2] which receives less attention than it deserves is the converse of the above statement. That

is, when the possible states of the original system are linearly independent, then $1 \rightarrow N$ probabilistic cloning is possible for any $N \geq 1$. In this paper, we generalize this result to show that the linear independency of the original states is enough to make any information processing tasks possible in a probabilistic manner.

Another fundamental task in quantum computation and quantum information processing is quantum discrimination. Given that the system of interest is prepared in one of some possible states, the purpose of discrimination is to tell which state the system is actually in. Rather surprisingly, these two seemingly, at least at first glance, very different tasks are closely related. A quantum system can be perfectly cloned [3, 4] (resp. perfectly discriminated [5]) if and only if the possible states of the system are orthogonal; and it can be conclusively cloned [2] (resp. unambiguously discriminated [2, 6]) if and only if the possible states are linearly independent. Furthermore, Duan and Guo [2] pointed out that exact $1 \rightarrow \infty$ cloning and unambiguous discrimination can be simulated by each other; a more delicate and quantitative connection between these two tasks was investigated in Ref. [7].

Motivated by this connection, Chefles and Barnett proposed a generalized way, namely quantum separation, to deal with quantum exact cloning and quantum unambiguous discrimination uniformly [7]. To be specific, suppose a quantum system is prepared in one of the two states $|\psi_1\rangle$ and $|\psi_2\rangle$ but we do not know exactly which one. A quantum separation performed on this system then leads, generally in a probabilistic but conclusive manner, the system into $|\psi'_i\rangle$ provided that originally it is in the state $|\psi_i\rangle$, for $i = 1, 2$. In their paper, Chefles and Barnett put a constraint that the desired states $|\psi'_1\rangle$ and $|\psi'_2\rangle$ should satisfy the condition that

$$|\langle\psi'_1|\psi'_2\rangle| \leq |\langle\psi_1|\psi_2\rangle|, \quad (1)$$

just as in the cases of exact cloning and unambiguous discrimination. That is also why they called this process ‘separation’ since decrease of the inner product means that these two states become more distinct or separable. In the present paper, we generalize this concept in two

*Electronic address: feng-y@tsinghua.edu.cn

†Electronic address: dry02@mails.tsinghua.edu.cn

‡Electronic address: jizhengfeng98@mails.tsinghua.edu.cn

ways. First, we get rid of the constraint in Eq.(1) to consider more general physical processes, although we still use the term ‘separation’ for convenience. Second, we generalize separation to the case of multiple mixed states.

To be specific, we give the formal definition of quantum separation as follows. Suppose a quantum system is prepared in a state secretly chosen from ρ_1, \dots, ρ_n . A quantum separation is a physically realizable process which, generally in a probabilistic but conclusive manner, leads ρ_i to ρ'_i for some quantum states ρ'_1, \dots, ρ'_n . Recall that any physically realizable process is completely positive and trace preserving, and so can be represented by Kraus operator-sum form [8]. That is, there exist quantum operators A_{Sk}, A_{Fk} such that

$$A_{Sk}\rho_i A_{Sk}^\dagger = s_{ik}\rho'_i, \quad (2)$$

$$A_{Fk}\rho_i A_{Fk}^\dagger = f_{ik}\sigma_{ik} \quad (3)$$

for some nonnegative real numbers s_{ik} and f_{ik} , and mixed states σ_{ik} , where $i = 1, \dots, n$. Here the subscript S and F denote success and failure, respectively. Intuitively, Eq.(2) means that if the separation succeeds, the system evolves into ρ'_i provided that it is originally in the state ρ_i . Notice that there may be more than one operator, indexed by k , corresponding to successfully separating ρ_i or getting an inconclusive result. By appending the shorter group with zero operators, we can assume that the range of k is taken the same for success and failure. Furthermore, these operators should satisfy the completeness relation

$$\sum_k (A_{Sk}^\dagger A_{Sk} + A_{Fk}^\dagger A_{Fk}) = I. \quad (4)$$

Here I is the identity operator.

Since no constraints are put on the output states in the general framework, we can in fact represent any oblivious computation and information process by quantum state separation. To see the power of this framework more explicitly, let us examine some special cases. It is easy to check that exact $1 \rightarrow N$ cloning is a special case of quantum separation by letting the desired state ρ'_i be $\rho_i^{\otimes N}$ while unambiguous discrimination is the case when all ρ'_i are orthogonal such that there exists a quantum measurement which can further discriminate them perfectly. Furthermore, suppose all ρ_i lie in a Hilbert space \mathcal{H} . The $1 \rightarrow N$ mixed state broadcasting [9] can be involved in the general framework of quantum state separation by requiring that each ρ'_i lies in the Hilbert space $\mathcal{H}^{\otimes N}$ and the reduced density matrices of ρ'_i obtained by tracing over any $N - 1$ subsystems equal to ρ_i . Note also that unambiguous filtering [10], unambiguous comparison [11], and unambiguous subset discrimination [12] are all special cases of unambiguous discrimination between mixed states, which has received much attention in recent years [13-19]. By considering quantum state separation, we can deal with all these information processing processes in a uniform and more general way.

The aim of this paper is to examine the conditions and the capability of quantum information processing in the framework of state separation. In Sec. II, we show that in order to physically realize a universal and conclusive information processing task on an unknown system, linearity is in fact the only constraint. In other words, when the possible states of the unknown system are linearly independent, then any separation with any output states is possible. In Sec. III, we derive a lower bound on the average failure probability of any physically realizable quantum separation, when the mixed state case is considered.

II. CONDITIONS OF STATE SEPARATION

In this section, we derive some necessary and sufficient conditions for quantum separation to be physically realizable. First, when the final states are specified, we have the following theorem for the pure state case.

Theorem 1 *Given two sets of pure states $|\psi_1\rangle, \dots, |\psi_n\rangle$ and $|\psi'_1\rangle, \dots, |\psi'_n\rangle$. There exists a quantum separation which can lead $|\psi_i\rangle$ to $|\psi'_i\rangle$ if and only if*

$$X - \sqrt{\Gamma}X'\sqrt{\Gamma} \geq 0 \quad (5)$$

for some positive definite diagonal matrix $\Gamma = \text{diag}(\gamma_1, \dots, \gamma_n)$, where $n \times n$ matrices $X = [\langle\psi_i|\psi_j\rangle]$ and $X' = [\langle\psi'_i|\psi'_j\rangle]$. Here by $M \geq 0$ we mean that the matrix M is positive semidefinite, i.e., for any n -dimensional complex vector α , $\alpha M \alpha^\dagger \geq 0$.

To prove this theorem, we introduce first a lemma proven in Ref. [2]:

Lemma 1 *For any two sets of pure states $|\psi_1\rangle, \dots, |\psi_n\rangle$ and $|\psi'_1\rangle, \dots, |\psi'_n\rangle$, if*

$$\langle\psi_i|\psi_j\rangle = \langle\psi'_i|\psi'_j\rangle \quad (6)$$

for any $i, j = 1, \dots, n$, then there exists a unitary operator U such that $U|\psi_i\rangle = |\psi'_i\rangle$.

We learn from this lemma that in pure state case, the only thing determining whether or not there exists a unitary evolution between two sets of states is the inner products of all pairs of states from the same set. This is a remarkable property of pure state evolution. When mixed states are considered, things become more complicated and many more facts other than fidelities between different states must be involved to determine the existence of such a unitary transformation. That is also why we consider only pure state case here.

Having the above lemma as a tool, we can prove Theorem 1 as follows:

Proof of Theorem 1. By definition, there exist quantum operators A_{Sk} and A_{Fk} satisfying Eq.(4) such that

$$A_{Sk}|\psi_i\rangle = \sqrt{s_{ik}}|\psi'_i\rangle \quad (7)$$

$$A_{Fk}|\psi_i\rangle = \sqrt{f_{ik}}|\phi_{ik}\rangle, \quad (8)$$

for some state $|\phi_{ik}\rangle$, where $0 < s_{ik} \leq 1$ and $0 \leq f_{ik} < 1$. For any n -dimensional complex vector $\alpha = (\alpha_1, \dots, \alpha_n)$, let $|\Psi\rangle = \sum_{i=1}^n \alpha_i |\psi_i\rangle$. Notice that $A_{Fk}^\dagger A_{Fk}$ is positive semidefinite for any k . It follows that

$$\begin{aligned} 0 &\leq \langle \Psi | \sum_k A_{Fk}^\dagger A_{Fk} | \Psi \rangle \\ &= \langle \Psi | I - \sum_k A_{Sk}^\dagger A_{Sk} | \Psi \rangle \\ &= \langle \Psi | \Psi \rangle - \sum_k \langle \Psi | A_{Sk}^\dagger A_{Sk} | \Psi \rangle \\ &= \sum_{i,j} \alpha_i^* \alpha_j \langle \psi_i | \psi_j \rangle - \sum_k \sum_{i,j} \alpha_i^* \alpha_j \sqrt{s_{ik} s_{jk}} \langle \psi'_i | \psi'_j \rangle \\ &= \alpha X \alpha^\dagger - \alpha \sum_k \sqrt{S_k} X' \sqrt{S_k}^\dagger \\ &\leq \alpha X \alpha^\dagger - \alpha \sqrt{S_1} X' \sqrt{S_1}^\dagger. \end{aligned} \quad (9)$$

Here, $S_k = \text{diag}(s_{1k}, \dots, s_{nk})$ are $n \times n$ diagonal matrices. The last line of Eq.(9) follows from the fact that for any k , $\sqrt{S_k} X' \sqrt{S_k}$ is positive semidefinite. From the arbitrariness of α , we derive that

$$X - \sqrt{S_1} X' \sqrt{S_1}^\dagger \geq 0, \quad (10)$$

which completes the proof of the necessity part.

The proof of the sufficiency part is almost the same as the proof of that linear independency implies capability of exact cloning in Ref. [2]. To be complete, we outline here the main steps.

To show the existence of a desired separation under the assumption of Eq.(5), we need only to prove that there exists a unitary transformation U such that for any $i = 1, \dots, n$,

$$U|\psi_i\rangle_A |\Sigma\rangle_B |P\rangle_P = \sqrt{\gamma_i} |\psi'_i\rangle_{AB} |P_0\rangle_P + \sum_{k=1}^n c_{ik} |\Phi_i\rangle_{AB} |P_k\rangle_P, \quad (11)$$

where $|P_0\rangle, |P_1\rangle, \dots, |P_n\rangle$ are orthonormal states in the probe system P , and $|\Phi_i\rangle_{AB}$ are normalized but not necessarily orthogonal states. Here the subscript B denotes an ancillary system and $|\Sigma\rangle$ is a standard 'blank' state (in some cases, say unambiguous discrimination, the ancillary system is unnecessary). After the unitary evolution described by Eq.(11), a projective measurement which consists of $|P_0\rangle\langle P_0|$ and $I - |P_0\rangle\langle P_0|$ is performed on probe system P . If the outcome corresponding to $I - |P_0\rangle\langle P_0|$ occurs, the separation fails; otherwise this separation succeeds and the secretly chosen state $|\psi_i\rangle$ conclusively evolves into the desired state $|\psi'_i\rangle$.

In the following, we show the existence of the unitary transformation U in Eq.(11). Taking the inter-inner

products of the both sides of Eq.(11) for different i and j , we have the matrix equation

$$X = \sqrt{\Gamma} X' \sqrt{\Gamma} + C C^\dagger, \quad (12)$$

where $n \times n$ matrix $C = [c_{ij}]$. From Lemma 1, the only thing left is to show the existence of the matrix C . But from Eq.(5), the positive semidefinite matrix $X - \sqrt{\Gamma} X' \sqrt{\Gamma}$ can be diagonalized by a unitary matrix V as

$$V(X - \sqrt{\Gamma} X' \sqrt{\Gamma})V^\dagger = \text{diag}(c_1, \dots, c_n) \quad (13)$$

for some nonnegative numbers c_1, \dots, c_n . So we need only set $C = V^\dagger \text{diag}(\sqrt{c_1}, \dots, \sqrt{c_n})V^\dagger$ and then the sufficiency part of the theorem is proven. ■

Theorem 1 tells us when a *given* separation can be physically realized in pure state case. The following theorem, however, gives a necessary and sufficient condition under which *any* quantum separation is realizable on a given system in the general case of mixed states. To begin with, we introduce some notations. For a density matrix ρ , we denote by $\text{supp}(\rho)$ the support space of ρ . That is, the space spanned by all eigenvectors with nonzero corresponding eigenvalues of ρ . Furthermore, by $\text{supp}(\rho_1, \dots, \rho_n)$ we denote the support space spanned by eigenvectors of ρ_1, \dots, ρ_n with nonzero corresponding eigenvalues.

Theorem 2 Suppose a quantum system is prepared in a state secretly chosen from ρ_1, \dots, ρ_n . Let $S = \{\rho_1, \dots, \rho_n\}$ and $S_i = S \setminus \{\rho_i\}$. Then

1) any state separation on this system is possible (that is, for any states ρ'_1, \dots, ρ'_n , there exists a separation which leads ρ_i conclusively to ρ'_i) if and only if $\text{supp}(S) \neq \text{supp}(S_i)$ for any $i = 1, \dots, n$.

2) Furthermore, if $\text{supp}(S) = \text{supp}(S_i)$ for some i and there exists a separation which leads ρ_i conclusively to ρ'_i for some quantum states ρ'_1, \dots, ρ'_n , then $\text{supp}(S') = \text{supp}(S'_i)$, where $S' = \{\rho'_1, \dots, \rho'_n\}$ and $S'_i = S' \setminus \{\rho'_i\}$.

Proof. The necessity part of 1) is obvious, since we can take special cases of quantum separation, say unambiguous discrimination, to show that $\text{supp}(S) \neq \text{supp}(S_i)$ (for the condition under which unambiguous discrimination between mixed states is possible, we refer to Ref. [18]).

To prove the sufficiency part of 1), suppose that $\text{supp}(S) \neq \text{supp}(S_i)$ for any $i = 1, \dots, n$. Then from Ref. [18], there exist n positive real numbers $\gamma_1, \dots, \gamma_n$ such that we can unambiguously discriminate ρ_i with probability γ_i . Once the state ρ_i is identified, we can prepare ρ'_i with certainty by a physical realizable process (which may be dependent on ρ'_i). So by combining these two steps together, we construct a protocol which leads ρ_i to ρ'_i with positive probability γ_i .

Now we prove 2) by contradiction. Suppose $\text{supp}(S') \neq \text{supp}(S'_i)$. Then there exists a pure state $|\phi\rangle$ which is in $\text{supp}(\rho_i)$ but not in $\text{supp}(S'_i)$. So we can construct a positive-operator valued measurement comprising $|\phi\rangle\langle\phi|$

and $I - |\phi\rangle\langle\phi|$ to unambiguously discriminate ρ_i from the other $n-1$ states with a positive probability. Notice that an unambiguous discrimination is also a quantum separation. Combining these two separation processes together we get a new one which can discriminate unambiguously the state ρ_i from other states with a positive probability. That is a contradiction with the assumption that $\text{supp}(S) = \text{supp}(S_i)$. ■

Notice that when $\rho_1 = |\psi_1\rangle\langle\psi_1|, \dots, \rho_n = |\psi_n\rangle\langle\psi_n|$ are all pure states, the condition that $\text{supp}(S) \neq \text{supp}(S_i)$ for any $i = 1, \dots, n$ is equivalent to that $|\psi_1\rangle, \dots, |\psi_n\rangle$ are linearly independent. So we have the following corollary which has more physical intuition.

Corollary 1 *Suppose a quantum system is prepared secretly in one of the states $|\psi_1\rangle, \dots, |\psi_n\rangle$. Then*

1) *any state separation on this system is possible if and only if $|\psi_1\rangle, \dots, |\psi_n\rangle$ are linearly independent.*

2) *Furthermore, if $|\psi_1\rangle, \dots, |\psi_n\rangle$ are linearly dependent and there exists a separation which leads $|\psi_i\rangle$ conclusively to $|\psi'_i\rangle$ for some quantum states $|\psi'_1\rangle, \dots, |\psi'_n\rangle$, then $|\psi'_1\rangle, \dots, |\psi'_n\rangle$ are also linearly dependent.*

The two statements in Corollary 1 are complementary with each other. Statement 2) tells us the constraints on realizable information processing tasks when the system we are concerned with is in a state coming secretly from a linearly dependent set. On the other hand, statement 1) shows that linear dependency is actually the only case in which physically realizable information processing tasks will be constrained. That is, if the state of the original system is prepared secretly in one of linearly independent pure states, then any tasks, represented by our generalized separation with arbitrary outcome states, are probabilistically and conclusively realizable.

From Theorem 1, we get the following direct corollary:

Corollary 2 *For any set $S = \{\rho_1, \dots, \rho_n\}$ of quantum states, the following statements are equivalent:*

1) *The states secretly chosen from S can be unambiguously discriminated.*

2) *The states secretly chosen from S can be conclusively cloned.*

3) *The set S can evolve, through appropriate separation processes, into any set $S' = \{\rho'_1, \dots, \rho'_n\}$ of quantum states, where ρ_i becomes ρ'_i for any $i = 1, \dots, n$.*

Informally, from this corollary, exact cloning and unambiguous discrimination put the strongest constraints on the possible states the original system can be prepared in.

III. LOWER BOUND ON AVERAGE FAILURE PROBABILITY

Theorem 1 gives a necessary and sufficient condition under which a given separation can be realized for a given original system, when the case of pure state is considered.

The general case where the state of the system we are concerned with comes from a mixed state set is, however, not investigated. Actually, it is unlikely that there exists a corresponding condition for mixed states due to lack of a result similar to Lemma 1. However, we can still derive a lower bound on the average failure probability of any separation once it is realizable.

Theorem 3 *Suppose a quantum system is prepared in a state secretly chosen from ρ_1, \dots, ρ_n with respective a priori probabilities η_1, \dots, η_n , and there exists a separation which leads ρ_i to ρ'_i for some quantum states ρ'_1, \dots, ρ'_n . Then the average failure probability P_f of this separation satisfies*

$$P_f \geq \sqrt{\frac{n}{n-1} \sum_{(i,j) \in \Delta} \eta_i \eta_j \left(\frac{F(\rho_i, \rho_j) - F(\rho'_i, \rho'_j)}{1 - F(\rho'_i, \rho'_j)} \right)^2}, \quad (14)$$

where the index set $\Delta = \{(i, j) : i \neq j \text{ and } F(\rho'_i, \rho'_j) \leq F(\rho_i, \rho_j)\}$.

Proof. From the assumption, there exist quantum operators A_{Sk} and A_{Fk} satisfying the completeness relation Eq.(4), such that Eqs.(2) and (3) hold. It is easy to check that

$$P_f = \sum_{i,k} \eta_i f_{ik} \quad (15)$$

and for any $i = 1, \dots, n$,

$$\sum_k (s_{ik} + f_{ik}) = 1. \quad (16)$$

By Cauchy-Schwarz inequality,

$$\begin{aligned} P_f^2 &\geq \frac{n}{n-1} \sum_{i \neq j} \eta_i \eta_j \left(\sum_k f_{ik} \right) \left(\sum_k f_{jk} \right) \\ &\geq \frac{n}{n-1} \sum_{i \neq j} \eta_i \eta_j \left(\sum_k \sqrt{f_{ik} f_{jk}} \right)^2. \end{aligned} \quad (17)$$

From Eq.(2) and Polar decomposition theorem, we have

$$A_{Sk} \sqrt{\rho_i} = \sqrt{A_{Sk} \rho_i A_{Sk}^\dagger} U_{ik} = \sqrt{s_{ik}} \sqrt{\rho'_i} U_{ik} \quad (18)$$

for some unitary matrix U_{ik} . And similarly, Eq.(3) implies that

$$A_{Fk} \sqrt{\rho_i} = \sqrt{A_{Fk} \rho_i A_{Fk}^\dagger} V_{ik} = \sqrt{f_{ik}} \sqrt{\sigma_{ik}} V_{ik} \quad (19)$$

for some unitary matrix V_{ik} .

Recall that for any density matrices ρ and σ , the fidelity $F(\rho, \sigma) = \max_U |\text{Tr}(\sqrt{\rho} \sqrt{\sigma} U)|$, where the maximum is taken over all unitary matrix U . For any $i \neq j$, let us take U_i^j such that $F(\rho_i, \rho_j) = |\text{Tr}(\sqrt{\rho_i} \sqrt{\rho_j} U_i^j)|$. Then

$$\text{Tr}(\sqrt{\rho_i} A_{Sk}^\dagger A_{Sk} \sqrt{\rho_j} U_i^j) = \sqrt{s_{ik} s_{jk}} \text{Tr}(U_{ik}^\dagger \sqrt{\rho'_i} \sqrt{\rho'_j} U_{jk} U_i^j) \quad (20)$$

$$\text{Tr}(\sqrt{\rho_i} A_{Fk}^\dagger A_{Fk} \sqrt{\rho_j} U_i^j) = \sqrt{f_{ik} f_{jk}} \text{Tr}(V_{ik}^\dagger \sqrt{\sigma_{ik}} \sqrt{\sigma_{jk}} V_{jk} U_i^j). \quad \text{and} \quad (21)$$

Summing up Eqs.(20) and (21) for all k and noticing Eq.(4), we have

$$F(\rho_i, \rho_j) = \left| \sum_k (\sqrt{s_{ik} s_{jk}} \text{Tr}(\sqrt{\rho'_i} \sqrt{\rho'_j} W_{ijk}) + \sqrt{f_{ik} f_{jk}} \text{Tr}(\sqrt{\sigma_{ik}} \sqrt{\sigma_{jk}} W'_{ijk})) \right|, \quad (22)$$

where $W_{ijk} = U_{jk} U_i^\dagger U_{ik}^\dagger$ and $W'_{ijk} = V_{jk} U_i^j V_{ik}^\dagger$ are unitary matrices. We further derive that

$$\begin{aligned} F(\rho_i, \rho_j) &\leq \sum_k \sqrt{s_{ik} s_{jk}} |\text{Tr}(\sqrt{\rho'_i} \sqrt{\rho'_j} W_{ijk})| \\ &\quad + \sum_k \sqrt{f_{ik} f_{jk}} |\text{Tr}(\sqrt{\sigma_{ik}} \sqrt{\sigma_{jk}} W'_{ijk})| \\ &\leq \sum_k \sqrt{s_{ik} s_{jk}} F(\rho'_i, \rho'_j) \\ &\quad + \sum_k \sqrt{f_{ik} f_{jk}} F(\sigma_{ik}, \sigma_{jk}) \\ &\leq \sum_k \sqrt{s_{ik} s_{jk}} F(\rho'_i, \rho'_j) + \sum_k \sqrt{f_{ik} f_{jk}}. \end{aligned} \quad (23)$$

Notice that

$$\begin{aligned} \sum_k \sqrt{s_{ik} s_{jk}} &\leq \sum_k \frac{s_{ik} + s_{jk}}{2} \\ &= 1 - \sum_k \frac{f_{ik} + f_{jk}}{2} \\ &\leq 1 - \sum_k \sqrt{f_{ik} f_{jk}}. \end{aligned} \quad (24)$$

Substituting Eq.(24) into Eq.(23), we have

$$\sum_k \sqrt{f_{ik} f_{jk}} \geq \frac{F(\rho_i, \rho_j) - F(\rho'_i, \rho'_j)}{1 - F(\rho'_i, \rho'_j)} \quad (25)$$

Taking Eq.(25) for $(i, j) \in \Delta$ back into Eq.(17) and noticing that $\sum_k \sqrt{f_{ik} f_{jk}} \geq 0$ for $(i, j) \notin \Delta$, we arrive at the desired bound,

$$P_f \geq \sqrt{\frac{n}{n-1} \sum_{(i,j) \in \Delta} \eta_i \eta_j \left(\frac{F(\rho_i, \rho_j) - F(\rho'_i, \rho'_j)}{1 - F(\rho'_i, \rho'_j)} \right)^2}. \quad (26)$$

That completes the proof. \blacksquare

Following the argument behind Theorem 3 in Ref. [18], we can derive a series of lower bounds on the average failure probability. For the sake of completeness, we outline the derivation as follows. Define

$$M_t = \sum_i \eta_i^{2t} \left(\sum_k f_{ik} \right)^{2t} \quad (27)$$

$$N_t = \sum_{i \neq j} \eta_i^t \eta_j^t \left(\sum_k f_{ik} \right)^t \left(\sum_k f_{jk} \right)^t. \quad (28)$$

Then $M_t = \sqrt{N_{2t} + M_{2t}}$ and by Cauchy inequality, $M_t \geq N_t/(n-1)$. So for any $r \geq 0$,

$$\begin{aligned} P_f^2 &= N_1 + M_1 = N_1 + \sqrt{N_2 + M_2} = \dots \\ &= N_1 + \sqrt{N_2 + \sqrt{\dots + \sqrt{N_{2r} + M_{2r}}}} \\ &\geq N_1 + \sqrt{N_2 + \sqrt{\dots + \sqrt{\frac{n}{n-1} N_{2r}}}} \end{aligned} \quad (29)$$

If we further define

$$C_t = \sum_{(i,j) \in \Delta} \eta_i^t \eta_j^t \left(\frac{F(\rho_i, \rho_j) - F(\rho'_i, \rho'_j)}{1 - F(\rho'_i, \rho'_j)} \right)^{2t}, \quad (30)$$

then from Eq.(25) and the fact that $\sum_k \sqrt{f_{ik} f_{jk}} \geq 0$ for $(i, j) \notin \Delta$, we have $N_t \geq C_t$. Consequently, the promised lower bounds on the average failure probability P_f can be derived as

$$P_f \geq P_f^{(r)} \doteq \sqrt{C_1 + \sqrt{\dots + \sqrt{\frac{n}{n-1} C_{2r}}}}. \quad (31)$$

The bound presented in Eq.(14) is just the special case of the above bounds when $r = 0$. Note that $P_f^{(0)} \leq P_f^{(1)} \leq \dots$ by Cauchy-Schwarz inequality. When r increases, the bound becomes better and better; and the limit when r tends to infinity is the best bound we can derive using this method.

Now let us analyze the bound in Eq.(14) carefully. First, note that when pure state separation is considered, Qiu obtained in Ref. [20] a lower bound on the average failure probability which reads

$$1 - \frac{1}{n-1} \sum_{i < j} \frac{\eta_i + \eta_j - 2\sqrt{\eta_i \eta_j} |\langle \psi_i | \psi_j \rangle|}{1 - |\langle \psi'_i | \psi'_j \rangle|}. \quad (32)$$

It is easy by using Cauchy-Schwarz inequality to check that our bound presented in Eq.(14) is better in general than the one in Eq.(32). On the other hand, in the case of $M \rightarrow N$ ($M \leq N$) exact cloning, where the original state and the final state are, respectively, $\rho_i^{\otimes M}$ and $\rho_i^{\otimes N}$ for $i = 1, \dots, n$, and so $F(\rho'_i, \rho'_j) \leq F(\rho_i, \rho_j)$ holds for any $i \neq j$. So we have actually derived a lower bound on the average failure probability of exact $M \rightarrow N$ cloning as

$$P_f^{EC} \geq \sqrt{\frac{n}{n-1} \sum_{i \neq j} \eta_i \eta_j \left(\frac{F(\rho_i, \rho_j)^M - F(\rho_i, \rho_j)^N}{1 - F(\rho_i, \rho_j)^N} \right)^2}. \quad (33)$$

When $\rho_i = |\psi_i\rangle\langle\psi_i|$ are pure states and $\eta_1 = \dots = \eta_n = 1/n$, this bound can be shown better than

$$1 - \frac{2}{n(n-1)} \sum_{i < j} \frac{1 - |\langle\psi_i|\psi_j\rangle|^M}{1 - |\langle\psi_i|\psi_j\rangle|^N}, \quad (34)$$

which was derived in Ref. [7]. Finally, in the case of unambiguous discrimination, where the final states ρ'_i are orthogonal to each other, the bound in Eq.(14) turns out to be

$$P_f^{UD} \geq \sqrt{\frac{n}{n-1} \sum_{i \neq j} \eta_i \eta_j F(\rho_i, \rho_j)^2}, \quad (35)$$

coinciding with that obtained in Ref. [18]. It is also worth noting that the bound can further degenerate to the Jaeger-Shimony bound $1 - 2\sqrt{\eta_1\eta_2}|\langle\psi_1|\psi_2\rangle|$ for two pure states [21] and the IDP bound $1 - |\langle\psi_1|\psi_2\rangle|$ for two pure states with equal *a priori* probabilities [22, 23, 24].

IV. CONCLUSION

To conclude, by deriving a necessary and sufficient condition for any quantum separation to be physically real-

izable, we show that in probabilistic manner, linearity is in fact the only one that restricts the physically realizable tasks. That is, when a system is prepared in a state secretly chosen from a linearly independent pure state set, then any generalized state separation is physically realizable with a positive probability. A lower bound on the average failure probability of any quantum state separation is also derived and special cases of this bound are analyzed.

The authors thank the colleagues in the Quantum Computation and Quantum Information Research Group for useful discussion. This work was partly supported by the Natural Science Foundation of China (Grant Nos. 60273003, 60433050, and 60305005). R. Duan acknowledges the financial support of Tsinghua University (Grant No. 052420003).

-
- [1] P. W. Shor, in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by Shafi Goldwasser (IEEE Computer Society Press, New York, 1994), p. 124.
 - [2] L. M. Duan, G. C. Guo, Phys. Rev. Lett. 80 4999 (1998).
 - [3] W. K. Wootters, W. H. Zurek, Nature 299, 802 (1982).
 - [4] D. Dieks, Phys. Lett. A 92, 271 (1982).
 - [5] C. W. Helstrom, Quantum Detection and Estimation Theory, New York: Academic, 1976.
 - [6] A. Chefles, Phys. Lett. A 239, 339 (1998).
 - [7] A. Chefles and S. M. Barnett, J. Phys. A: Math. Gen. 31 10097 (1998).
 - [8] K. Kraus, States, Effects and Operations: Fundamental Notions of Quantum Theory, Berlin: Springer (1983).
 - [9] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. 76, 2818 (1996).
 - [10] M. Takeoka, M. Ban, and M. Sasaki, Phys. Rev. A 68, 012307 (2003).
 - [11] S. M. Barnett, A. Chefles, and I. Jex, Phys. Lett. A 307, 189 (2003).
 - [12] S. Y. Zhang and M. S. Ying, Phys. Rev. A 65, 062322 (2002).
 - [13] Y. Sun, J. A. Bergou, and M. Hillery, Phys. Rev. A 66, 032315 (2002).
 - [14] T. Rudolph, R. W. Spekkens, P. S. Turner, Phys. Rev. A 68, 010301(R)(2003).
 - [15] P. Raynal, N. Lutkenhaus, S. J. van Enk, Phys. Rev. A 68, 022308 (2003).
 - [16] J. Fiurasek and M. Jezek, Phys. Rev. A 67, 012321 (2003).
 - [17] Y. C. Eldar, Phys. Rev. A 67, 042309 (2003).
 - [18] Y. Feng, R. Y. Duan and M. S. Ying, Phys. Rev. A 70, 012308 (2004).
 - [19] J. A. Bergou, U. Herzog, and M. Hillery, Phys. Rev. A 71, 042314 (2005).
 - [20] D. W. Qiu, J. Phys. A: Math. Gen. 35 6931-6937 (2002).
 - [21] G. Jaeger, A. Shimony, Phys. Lett. A 197, 83 (1995).
 - [22] I. D. Ivanovic, Phys. Lett. A 123, 257 (1987).
 - [23] D. Dieks, Phys. Lett. A 126, 303 (1988).
 - [24] A. Peres, Phys. Lett. A 128, 19 (1988).